2006 INTERNATIONAL CONTROL SYSTEMS SECURITY AND STANDARDS COORDINATION WORKSHOP

August 10-11, 2006
Portland, Oregon

Current Status of Japan's CIIP Guideline Development

Yoshizumi Serizawa

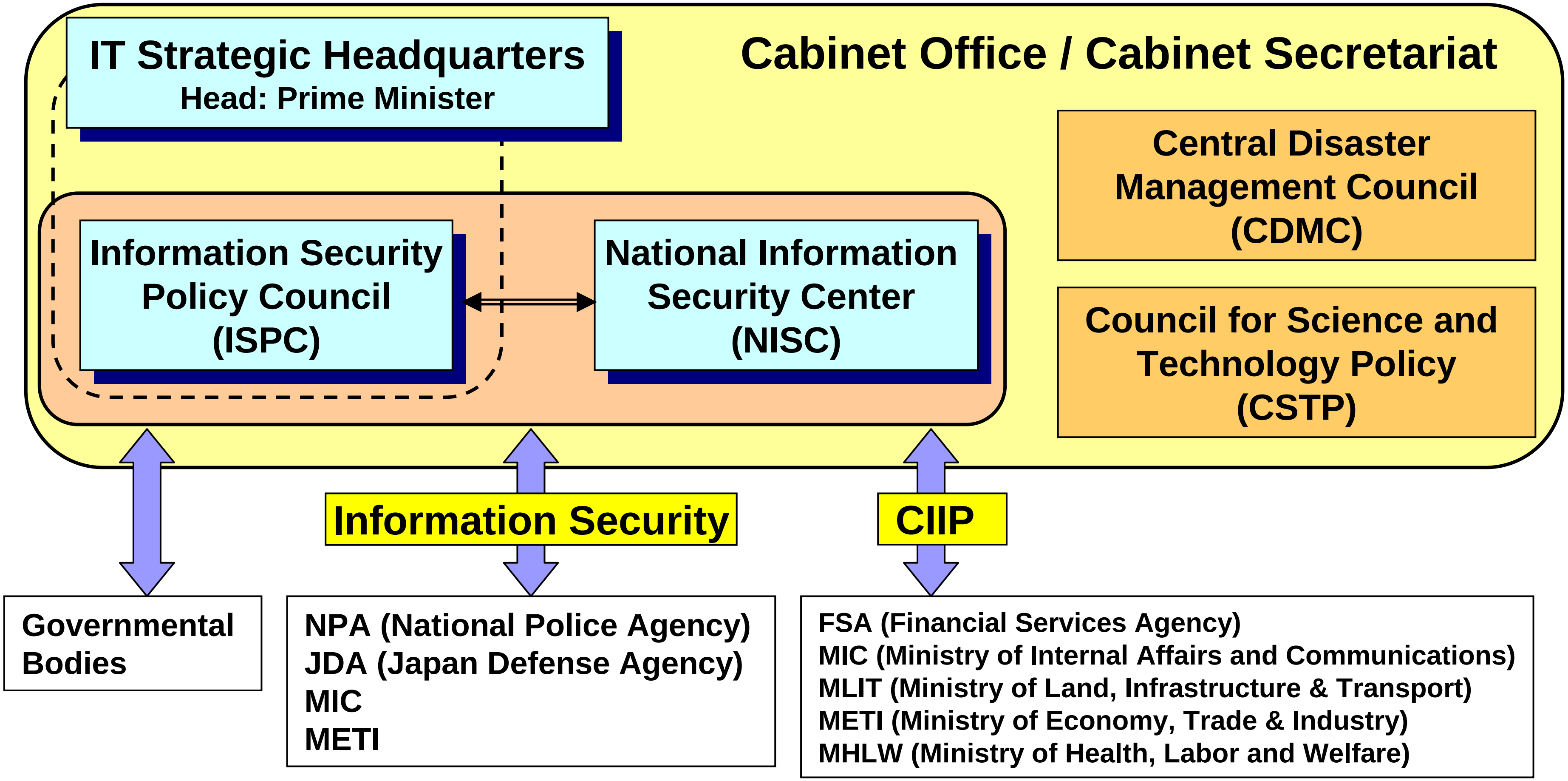
System Engineering Research Laboratory

Central Research Institute of Electric Power Industry

Outline

- Critical Infrastructures and Related Governmental Structure in Japan
- Action Plan on Information Security Measures for Critical Infrastructures
- Principles for Standard/Guideline Formulation
- Electricity Sector Activities

Government Structure for Information Security

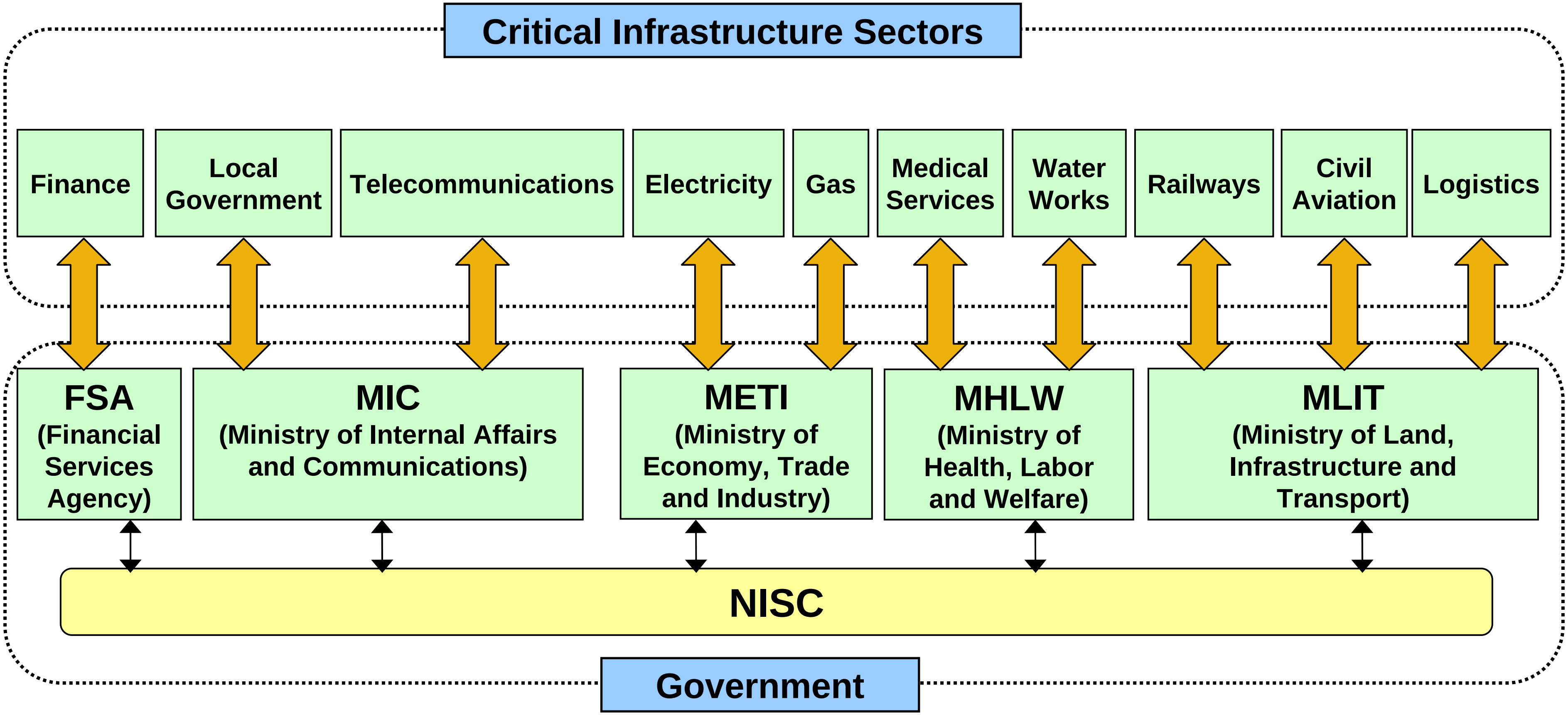


IT Strategic Headquarters
Head: Prime Minister
Cabinet Office / Cabinet Secretariat
Central Disaster Management Council (CDMC)
Council for Science and Technology Policy (CSTP)
Information Security Policy Council (ISPC)
National Information Security Center (NISC)
Information Security
CIIP
Governmental Bodies

NPA (National Police Agency)
JDA (Japan Defense Agency)
MIC
METI

FSA (Financial Services Agency)
MIC (Ministry of Internal Affairs and Communications)
MLIT (Ministry of Land, Infrastructure & Transport)
METI (Ministry of Economy, Trade & Industry)
MHLW (Ministry of Health, Labor and Welfare)

Critical Infrastructures


Critical Infrastructure Sectors
Finance
Local Government
Telecommunications
Electricity
Gas
Medical Services
Water Works
Railways
Civil Aviation
Logistics
FSA (Financial Services Agency)
MIC (Ministry of Internal Affairs and Communications)
METI (Ministry of Economy, Trade and Industry)
MHLW (Ministry of Health, Labor and Welfare)
MLIT (Ministry of Land, Infrastructure and Transport)
NISC
Government

Action Plans on CIIP

- "Special Action Plan on Countermeasures to Cyber-terrorism for Critical Infrastructures," December 2000
- "Basic Concept on Information Security Measures for Critical Infrastructures," adopted by the Information Security Policy Council on September 15, 2005
- "Action Plan on Information Security Measures for Critical Infrastructures," December 13, 2005, considering rapid spread of IT use and increased IT dependence in the critical infrastructure sectors as well as their growing interdependences

Action Plan on Information Security Measures for Critical Infrastructures

- To protect critical infrastructures from IT-malfunctions (suspended services and reduced function) caused by dysfunction of IT system arising from
  - □ Cyber attacks
  - □ Unintentional factors
  - □ Disasters
- Actions
  - □ Raising the information security level
  - □ Strengthening the information sharing frameworks
  - □ Analyzing interdependences
  - □ Implementing cross-sectoral exercises

Raising Information Security Level

- To formulate and reviews "Safety Standard, Guidelines, etc." on technical and operational standards
- "Principles for Formulation of 'Safety Standards, Guidelines, etc.' concerning Assurance of Information Security of Critical Infrastructures" formulated by NISC (National Information Security Center) by the end of FY 2005
- Promotes each infrastructure sector to clearly indicate the necessary or desirable standards for information security measures in its own "Safety Standard, Guidelines, etc." based on the above principles by around September 2006

Strengthening Information Sharing Frameworks

- To reorganize and strengthen existing information sharing frameworks, and increases the quantity and quality of the available information, prescribing in detail the systems of information sharing, liaison, and coordination between the public and private sectors, such as the liaison system used at times of IT-malfunctions
- Establishes an information-sharing organization, CEPTOAR (tentative), a kind of ISAC (Information Sharing and Analysis Center), in each critical infrastructure sector by the end of FY 2006
- Promotes cross-sectoral information sharing, establishing e.g. “CEPTOAR-Council”

CEPTOR: Capability for Engineering of Protection,
Technical Operation, Analysis and Response

Analyzing Interdependences

- To conduct cross-sectoral status assessment, or interdependence analysis, of the critical infrastructures under the initiative of NISC
- Outlines the effects and implementation procedure of analysis of interdependence
- Starts trial analyses of interdependence under the initiative of NISC in FY 2006

Implementing Cross-sectoral Exercises

- **To enforce fiscal-year-basis cross-sectoral exercises with concrete threat scenarios corresponding to the assumed threats**
- **Draws up “Exercise Implementation Plans” in the Cabinet Secretariat**
- **Conducts “Exercises for Research” and “Tabletop Exercises” in FY 2006, and “Functional Exercises” in FY 2007, with participation from respective critical infrastructures under the supervision of NISC**

Principles for Formulation

I. Purpose and position

- For the assurance of information security of critical infrastructures
- Necessity for “Safety Standards, Guidelines, etc.”
- What is the “Safety Standards, Guidelines, etc.”?
- Position of the Principles
- Expectations for the formulation and revision of the “Safety Standards, Guidelines, etc.” based on the Principles

II. Items to be defined in the “Safety Standards, Guidelines, etc.”

- Scope of the “Safety Standards, Guidelines, etc.” and targeted threats
- Disclosure of the “Safety Standards, Guidelines, etc.”
- Detailed items

III. Follow-ups

- Reviewing the Principles (annually or as needed)
- Continuous verification of the “Safety Standards, Guidelines, etc.

Detailed Items

- Purpose for formulating the “Safety Standards, Guidelines, etc.”
- Targeted scope and assumed threats
- Respective roles of business entities engaged in critical infrastructures, etc.
- Targeted items
  - Four aspects for establishing security measures
    - Organizations/frameworks and resources
    - Information rating and handling
    - Information security requirements and threats
    - Information systems (facilities, environment, computers, software, communication systems, etc.)
  - Three prioritized items
    - Measures for ensuring business continuity when IT-malfunctions occur
    - Measures for preventing information leakage
    - Measures for ensuring information security upon outsourcing

References

- NISC

  http://www.nisc.go.jp/eng/index.html

- Action Plan on Information Security Measures for Critical Infrastructures

  http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pd

- Principles for Formulating of “Safety Standards, Guidelines, etc.” concerning Assurance of Information Security of Critical Infrastructures

  http://www.nisc.go.jp/eng/pdf/principles_ci_eng.pdf

Electricity Sector Activities

- Process to be improved
  - □ Preparation, prevention, and protection
  - □ Response and recovery
  - □ Exercise and evaluation for improvement
- Risks to be concerned
  - □ Cyber attacks, disasters, unintentional troubles,…
- Ten sectors working together

Electricity Sector

- ● Information sharing
- ● Security guidelines, policies
- ● Exercises, vulnerability assessment, etc.

Present Power Control System Guideline

- Laid down by FEPC (Federation of Electric Power Companies) for Japanese power companies, not disclosed to the public
- Describes high-level technical and operational baselines against cyber attacks in addition to disasters
- Rules physical configurations, network connections, access control, monitoring and logging, emergency response, system and data management, education, etc.
- Referred to for each power company’s specific rule

Thank you for your attention.

Yoshizumi Serizawa

System Engineering Research Laboratory

Central Research Institute of Electric Power Industry

E-mail: seri@criepi.denken.or.jp

Summary of Action Plan (1)

To protect critical infrastructures from IT-malfunctions (suspended services and reduced function) caused by dysfunction of IT arising from

- Cyber attacks
- Unintentional factors
- Disasters

- Safety Standards, Guidelines, etc.
  - Safety standard guidelines to be formulated by NISC in 2006
  - Safety standards to be formulated and reviewed for each sector by September 2006

Summary of Action Plan (2)

- Information Sharing Frameworks
  - □ Functions for information sharing and analysis to be developed for each sector by the end of FY 2006
  - □ Basic agreements to be made for the sectors of medical services, water works, and logistics by the end of FY 2006
- Interdependence Analysis
  - □ Trial analysis of interdependence to be started by NISC in FY 2006
- Cross-sectoral exercises
  - □ “Exercises for research” and “tabletop exercises” to be implemented by NISC in FY 2006
  - □ “Functional exercises” to be implemented NISC in FY 2007